Class field theory in Pari/GP

Aurel Page
Inria / Université de Bordeaux

02/06/2026
Clervaux, Luxembourg

Plan

Class field theory

Goal

Let F be a number field.

Ultimate goal: classify all Galois extensions K/F and their Galois groups.

Reasonable goal (class field theory): classify all Galois extensions K/F with **abelian** Galois group.

Frobenius elements

Let K/F be a Galois extension of number fields with Galois group G.

$\mathfrak{p}$ prime ideal of $\mathbb{Z}_F$ and $\mathfrak{P} \mid \mathfrak{p}\mathbb{Z}_K$ prime ideal.
All other $\mathfrak{P}' \mid \mathfrak{p}\mathbb{Z}_K$ are $\mathfrak{P}' = \mathfrak{P}^\sigma$ for $\sigma \in G$.

If $\mathfrak{p}$ is unramified, there exist a **Frobenius element** $\mathrm{Frob}_\mathfrak{P} \in G$ such that for all $\alpha \in \mathbb{Z}_K$ we have

$$\mathrm{Frob}_\mathfrak{P}(\alpha) = \alpha^{N(\mathfrak{p})} \bmod \mathfrak{P}.$$

As $\mathfrak{P}'$ varies, the $\mathrm{Frob}_{\mathfrak{P}'}$ form a conjugacy class $\mathrm{Frob}_\mathfrak{p}$.

Example: cyclotomic fields

Let $K = \mathbb{Q}(\zeta_m)$, Galois over $\mathbb{Q}$ with Galois group $G \cong (\mathbb{Z}/m\mathbb{Z})^\times$:

$$\sigma_a : \zeta_m \mapsto \zeta_m^a \text{ for } a \in (\mathbb{Z}/m\mathbb{Z})^\times.$$

Let p be a prime number not dividing m, so that p is unramified in K, and let $\mathfrak{P}$ be a prime dividing $p\mathbb{Z}_K$.

Since G is abelian, Frob_p is a well-defined element of G.

We have (tautologically!)

$$\zeta_m^p = \zeta_m^p \bmod \mathfrak{P}.$$

Therefore $\mathrm{Frob}_p = \sigma_p$.

Kronecker–Weber theorem

Case $F = \mathbb{Q}$ of class field theory.

Theorem

Let $K/\mathbb{Q}$ be a Galois extension with abelian Galois group. Then there exists m such that

$$K \subset \mathbb{Q}(\zeta_m).$$

By Galois theory, there exists a subgroup $H \subset (\mathbb{Z}/m\mathbb{Z})^\times$ such that

$$K = \mathbb{Q}(\zeta_m)^H \text{ and } \mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times/H.$$

Modulus

We need a generalisation of $(\mathbb{Z}/m\mathbb{Z})^\times$ to other number fields F.

A **modulus** of F is a pair $\mathfrak{M} = (\mathfrak{M}_f, \mathfrak{M}_\infty)$ where

- $\mathfrak{M}_f$ is a nonzero ideal of $\mathbb{Z}_F$, and
- $\mathfrak{M}_\infty$ a set of real embeddings of F.

Let $\mathfrak{M}$ be a modulus of F. Let $\alpha \in F^\times$. We write

$$\alpha =^* 1 \bmod \mathfrak{M}$$

- if $v_\mathfrak{p}(\alpha - 1) \geq v_\mathfrak{p}(\mathfrak{M}_f)$ for all $\mathfrak{p}$ dividing $\mathfrak{M}_f$, and
- $\sigma(\alpha) > 0$ for every $\sigma \in \mathfrak{M}_\infty$.

Define

$$(\mathbb{Z}_F/\mathfrak{M})^\times = (\mathbb{Z}_F/\mathfrak{M}_f)^\times \times \{\pm 1\}^{\mathfrak{M}_\infty}.$$

Ray class groups

The **ray class group** of modulus $\mathfrak{M}$ is

$$\mathrm{Cl}_F(\mathfrak{M}) = \frac{(\text{fractional ideals coprime to } \mathfrak{M}_f)}{(\text{ideals } \alpha\mathbb{Z}_F \text{ with } \alpha =^* 1 \bmod \mathfrak{M})}.$$

This is a finite abelian group, and we have an exact sequence

$$1 \longrightarrow (\mathbb{Z}_F/\mathfrak{M})^\times/\mathbb{Z}_F^\times \longrightarrow \mathrm{Cl}_F(\mathfrak{M}) \longrightarrow \mathrm{Cl}_F \longrightarrow 1.$$

Example: $\mathrm{Cl}_{\mathbb{Q}}(m\infty) = (\mathbb{Z}/m\mathbb{Z})^\times$, $\mathrm{Cl}_{\mathbb{Q}}(m) = (\mathbb{Z}/m\mathbb{Z})^\times/\{\pm 1\}$.

Ray class fields

Theorem

Let F be a number field and $\mathfrak{M}$ a modulus. There exists a unique Galois extension $F(\mathfrak{M})$ of F, called the ***ray class field*** *of modulus $\mathfrak{M}$ such that the extension $F(\mathfrak{M})/F$ is unramified away of the primes dividing $\mathfrak{M}_f$, and such that the map*

$$\mathrm{Cl}_F(\mathfrak{M}) \longrightarrow \mathrm{Gal}(F(\mathfrak{M})/F)$$

defined by $\mathfrak{p} \mapsto \mathrm{Frob}_{\mathfrak{p}}$ is well-defined and is an isomorphism.

Example: $\mathbb{Q}(m\infty) = \mathbb{Q}(\zeta_m)$, $\mathbb{Q}(m) = \mathbb{Q}(\zeta_m)^+ = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$.

Exhaustivity

Theorem

Let K/F be a Galois extension with abelian Galois group. Then there exists $\mathfrak{M}$ such that

$$K \subset F(\mathfrak{M}).$$

By Galois theory, there exists a subgroup $H \subset \mathrm{Cl}_F(\mathfrak{M})$ such that

$$K = F(\mathfrak{M})^H \text{ and } \mathrm{Gal}(K/F) \cong \mathrm{Cl}_F(\mathfrak{M})/H.$$

Algorithms

Buchmann's algorithm

Goal: given a number field F, compute Cl_F.

Let S be a set of primes of F. The group $\mathbb{Z}_{F,S}^{\times}$ of **S-units** of F is the set of elements $\alpha \in F^{\times}$ such that $v_{\mathfrak{p}}(\alpha) = 0$ for all $\mathfrak{p} \notin S$.

Algorithm:

1. Choose S set of primes generating Cl_F (GRH).
2. Find S-units $R \subset \mathbb{Z}_{F,S}^{\times}$ (**hard!**).
3. Compute $C = \mathbb{Z}^S / \langle R \rangle$ and $U = \ker(\langle R \rangle \to \mathbb{Z}^S)$.
4. Check if $\langle R \rangle = \mathbb{Z}_{F,S}^{\times}$ using class number formula.
5. Output C.

Computing class groups

Notation: absolute value of discriminant Δ_F, degree n.

Assuming GRH:

- Heuristic: complexity $\exp(\tilde{O}(\log \Delta_F)^\alpha)$ for $1/3 \leq \alpha \leq 2/3$. (rigorous version by de Boer–Pellet-Mary–Wesolowski)
- Practice: impossible for $n > 150$.

Some orders of magnitude:

- low degree: $n = 2$, $\Delta_F \sim 10^{154}$ (record);
- medium degree: $n = 20$, $\Delta_F \sim 10^{85}$ (a few hours);
- high degree: $n \sim 100$ (record 116, $\Delta_F \sim 10^{273}$).

Unconditionally: $\tilde{O}(\Delta_F^{1/2})$.

Computing ray class groups

Recall the exact sequence

$$1 \longrightarrow (\mathbb{Z}_F/\mathfrak{M})^\times/\mathbb{Z}_F^\times \longrightarrow \mathrm{Cl}_F(\mathfrak{M}) \longrightarrow \mathrm{Cl}_F \longrightarrow 1.$$

Algorithm (computing $\mathrm{Cl}_F(\mathfrak{M})$):

1. Compute Cl_F.
2. **Factor** $\mathfrak{M}_f$.
3. Compute $(\mathbb{Z}_F/\mathfrak{M})^\times$ by Chinese Remainder Theorem.
4. Compute image of $\mathbb{Z}_F^\times$ in $(\mathbb{Z}_F/\mathfrak{M})^\times$ (**can be hard**).
5. Stitch together to obtain $\mathrm{Cl}_F(\mathfrak{M})$.

Discrete logarithm problem

Finite field $\mathbb{F}_q$, generator g of $\mathbb{F}_q^\times$.

Problem: given $h \in \mathbb{F}_q^\times$, compute $x \in \mathbb{Z}/(q-1)\mathbb{Z}$ such that

$$h = g^x.$$

Available algorithms:

- **generic**: complexity polynomial $\times \sqrt{\ell}$ where ℓ is the largest prime factor of $q-1$.
- **sieves** (NFS/FFS): complexity $\exp(\tilde{O}(\log q)^{1/3})$.
- very small characteristic: quasi-polynomial.

Kummer theory

Special case: assume $\zeta_\ell \in F$ for some integer ℓ.

Theorem

Let K/F be a Galois extension with $\mathrm{Gal}(K/F) \cong C_\ell$. Then there exists $\alpha \in F^\times$ such that $K = F(\alpha^{1/\ell})$.

More intrinsically:

$$\mathrm{Hom}(\mathrm{Gal}(\overline{F}/F), \mathbb{Z}/\ell\mathbb{Z}) \cong F^\times/(F^\times)^\ell.$$

Effective class field theory

Goal: computing the class field K corresponding to $G = \mathrm{Cl}_F(\mathfrak{M})/H$.

By splitting G into cyclic components C_ℓ, reduce to cyclic G.

Algorithm (case $\mathrm{Cl}_F(\mathfrak{M})/H \cong C_\ell$):

1. Compute $F_\ell = F(\zeta_\ell)$.
2. Choose appropriate set S of primes of F_ℓ.
3. Compute group U of S-units of F_ℓ (**as hard as class group of F_ℓ!**).
4. Find $\alpha \in U$ such that $K(\zeta_\ell) = F_\ell(\alpha^{1/\ell})$.
5. Descend $K(\zeta_\ell)/F_\ell$ to obtain K/F.

Norm relations

Using automorphisms

Question: assume F has a nontrivial group G of automorphisms. Can we use this to compute Cl_F faster?

- Use action of G to get extra S-units for free.
- Use structure of module over the group ring for faster linear algebra?
- By Galois theory, F has many subfields.

Examples: under GRH

- $F = \mathbb{Q}(\zeta_{6552})$
- $n = 1728$
- $\Delta_F = 2^{3456} \cdot 3^{2592} \cdot 7^{1440} \cdot 13^{1584} \approx 10^{5258}$
- $(\log \Delta_F)^2 \approx 10^8$

Cl_F computed in 4 hours on a laptop (single core).

- $\mathrm{rk}_2 \mathrm{Cl}_F = 112$
- $\mathrm{rk}_3 \mathrm{Cl}_F = 101$
- $h^+_{6552} = 70695077806080 = 2^{24} \cdot 3^3 \cdot 5 \cdot 7^4 \cdot 13 \approx 7 \cdot 10^{13}$

Examples: unconditionally

- $F = \mathbb{Q}(\zeta_{2520})$
- $n = 576$
- $\Delta_F = 2^{1152} \cdot 3^{864} \cdot 5^{432} \cdot 7^{480} \approx 10^{1466}$
- Minkowski bound $\approx 10^{515}$

Cl_F computed in 44 hours with a single core.

- $\mathrm{rk}_2\, \mathrm{Cl}_F = 38$
- $\mathrm{rk}_3\, \mathrm{Cl}_F = 15$
- $h^+_{2520} = 208 = 2^4 \cdot 13$

Notations

Notation for a set X: $\mathbb{Z}[X] = \bigoplus_{x \in X} \mathbb{Z}x$

Let G be a finite group: $\mathbb{Z}[G]$ is a ring.

A $\mathbb{Z}[G]$**-module** is an abelian group M with an action of G by linear automorphisms.

Notation: the group of **fixed points** is

$$M^G = \{m \in M \mid gm = m \text{ for all } g \in G\}.$$

Norm relations

For $H \leq G$, define the **norm element**

$$N_H = \sum_{h \in H} h \in \mathbb{Z}[G].$$

Wada, Bauch–Bernstein–de Valence–Lange–van Vredendaal, Biasse–van Vredendaal: $G = C_2 \times C_2 = \langle \sigma, \tau \rangle$.

$$2 = N_{\langle \sigma \rangle} + N_{\langle \sigma \rangle} - \sigma N_{\langle \sigma\tau \rangle}.$$

Parry, Lesavourey–Plantard–Susilo: $G = C_3 \times C_3 = \langle u, v \rangle$.

$$3 = N_{\langle u \rangle} + N_{\langle v \rangle} + N_{\langle uv \rangle} - (u + uv) N_{\langle u^2 v \rangle}.$$

Norm relations

A **norm relation** is an equality

$$d = \sum_{i=1}^{k} a_i N_{H_i} b_i$$

with $a_i, b_i \in \mathbb{Z}[G]$ and $d \in \mathbb{Z}_{>0}$.

Proposition

Let M be a $\mathbb{Z}[G]$-module. Then the exponent of

$$M/(\mathbb{Z}[G] \cdot M^{H_1} + \cdots + \mathbb{Z}[G] \cdot M^{H_k})$$

is finite and divides d.

Proof : Let $m \in M$. Then

$$dm = \sum_i a_i N_{H_i} b_i m \in \sum_i a_i M^{H_i}.$$

S-units

Apply to M the S-unit group of F:

The S-units of the subfields $F_i = F^{H_i}$ generate a $\mathbb{Z}[G]$-submodule of finite index in the S-units of F.

Algorithm (S-units with a norm relation):

1. For each subfield $F_i = F^{H_i}$, compute S-unit group $\mathbb{Z}_{F_i,S}^{\times}$.
2. Compute $\mathbb{Z}[G]$-module generated by all $\mathbb{Z}_{F_i,S}^{\times}$.
3. Extract all possible d-th powers to obtain $\mathbb{Z}_{F,S}^{\times}$.
4. Output $\mathbb{Z}_{F,S}^{\times}$.

Reduction to the subfields

Theorem (Biasse–Fieker–Hofmann–P.)

Assume GRH. Let G be a group admitting a norm relation. For any F with an action of G the computation of $\mathbb{Z}_{F,S}^{\times}$ reduces in polynomial time to the computation of $\mathbb{Z}_{F_1,S}^{\times}, \ldots, \mathbb{Z}_{F_k,S}^{\times}$.

Existence of norm relations

When do such relations exist?

Theorem

A finite group G admits a norm relation if and only if G contains

- *a non-cyclic subgroup of order pq (p,q, primes not necessarily distinct), or*
- *a subgroup isomorphic to $\mathrm{SL}_2(\mathbb{F}_p)$ where $p = 2^{2^k} + 1$ is a Fermat prime with $k > 1$.*

Takeaway: G is "**far from cyclic**".

Back to the example

- $K = \mathbb{Q}(\zeta_{6552})$
- $n = 1728$
- Galois group $G \cong C_{12} \times C_6^2 \times C_2^2$
- Relation with $d = 1$ reducing to 62 subfields of degree ≤ 192.
- Relations with d a power of 2 or 3 reducing to 672 subfields of degree ≤ 12.

Without automorphisms?

Question: What if F has no automorphisms?

- F has a Galois closure $\tilde{F}$ with a large automorphism group $G = \mathrm{Gal}(\tilde{F}/\mathbb{Q})$. Can we use this?
- $\tilde{F}$ has many subfields.
- On F, what remains of the action of G on $\tilde{F}$?

Hecke operators of finite groups

Let $H \subset G$ be a subgroup.

We have an isomorphism

$$\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G/H], M) \cong M^H$$

given by $\varphi \mapsto \varphi(1 \cdot H)$.

This gives the **Hecke ring**

$$\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G/H], \mathbb{Z}[G/H]) \cong \mathbb{Z}[G/H]^H \cong \mathbb{Z}[H\backslash G/H].$$

For every $T \in \mathbb{Z}[H\backslash G/H]$, we get a **Hecke operator**

$$T\colon M^H \longrightarrow M^H$$

by precomposition.

Galois theory and Hecke operators

For every F:

- the Galois group G acts on the Galois closure $\tilde{F}$, and
- there is a subgroup $H \subset G$ such that $F = \tilde{F}^H$.

If $U \subset G$ is a subgroup, **Hecke operators** T give morphisms

$$T : (\tilde{F}^U)^\times \longrightarrow (\tilde{F}^H)^\times = F^\times.$$

More precisely, morphisms of algebraic groups

$$T : \operatorname{Res}_{\tilde{F}^U/\mathbb{Q}} \mathbb{G}_m \longrightarrow \operatorname{Res}_{F/\mathbb{Q}} \mathbb{G}_m.$$

Generalised norm relations and S-units

Definition

G a finite group, subgroups $H \subset G$ and $U_1, \ldots, U_k \subset G$. Say that G admits a **norm relation** with respect to $(U_1, \ldots, U_k; H)$ if there exists a surjective morphism of $\mathbb{Q}[G]$-modules

$$\bigoplus_i \mathbb{Q}[G/U_i]^{n_i} \longrightarrow \mathbb{Q}[G/H].$$

Proposition

If there is such a norm relation, then the image under Hecke operators of

$$\mathbb{Z}_{F_1,S}^{\times}, \ldots, \mathbb{Z}_{F_k,S}^{\times}$$

has ***finite index*** *in* $\mathbb{Z}_{F,S}^{\times}$*, where* $F_i = \tilde{F}^{U_i}$.

Algorithmic consequence

Theorem (Étienne)

Assume GRH. If there is a norm relation, then the computation of $\mathbb{Z}_{F,S}^{\times}$ reduces in polynomial time to the computation of $\mathbb{Z}_{F_1,S}^{\times}, \ldots, \mathbb{Z}_{F_k,S}^{\times}$.

Questions ?

Thank you !